EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	7015	(transmit$4 or send$4 or receiv$4 or obtain$5 or forward$5) same (segment$4 or portion$4 or divid$4 or chop$3) same (duplicat$4 or replicat$4 or copy$4) same (concatenat$4 or link$4 or combin$4 or chain$4 or connect$4 or join$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/05/08 14:10
L2	14	(transmit$4 or send$4 or receiv$4 or obtain$5 or forward$5) same (segment$4 or portion$4 or divid$4 or chop$3) same (duplicat$4 or replicat$4 or copy$4) same (concatenat$4 or link$4 or combin$4 or chain$4 or connect$4 or join$4) same ((encrypt$4 or $2cipher$4 or scramb$4) near4 (different or multiple or plurality or second) near2 (key or method))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/05/08 14:22
L3	8	(transmit$4 or send$4 or receiv$4 or obtain$5 or forward$5) same (segment$4 or portion$4 or divid$4 or chop$3) same (duplicat$4 or replicat$4 or copy$4) same (concatenat$4 or link$4 or combin$4 or chain$4 or connect$4 or join$4) same ((encrypt$4 or $2cipher$4 or scramb$4) near4 ((different or multiple or plurality or second) near2 (key or method)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/05/08 14:14
L4	8	(transmit$4 or send$4 or receiv$4 or obtain$5 or forward$5) same (segment$4 or portion$4 or divid$4 or chop$3) same (duplicat$4 or replicat$4 or copy$4) same (concatenat$4 or link$4 or combin$4 or chain$4 or connect$4 or join$4) same ((encrypt$4 or $2cipher$4 or scramb$4) near4 ((different or multiple or plurality or second) near2 (key or method)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/05/08 14:14

EAST Search History

L5	151	(transmit$4 or send$4 or receiv$4 or obtain$5 or forward$5) same (segment$4 or portion$4 or divid$4 or chop$3) same (duplicat$4 or replicat$4 or copy$4) same (concatenat$4 or link$4 or combin$4 or chain$4 or connect$4 or join$4) and ((encrypt$4 or $2cipher$4 or scramb$4) near4 (different or multiple or plurality or second) near2 (key or method))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/05/08 15:35
L9	0	("5319712" "5754658" "6070245" "6448482" "20020083317" "20030002854" "6505299" "20030026423" "20030077071" "20030081776" "20030112333" "20030118243" "20030126086" "20030123664" "20030140257" "20030188154" "20030193973" "20030228018" "20040010717" "6684250" "20040028227" "20040081333" "20040091" "109" "20040193550" "20050071669" "6891565" "20050169473" "20050192904").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/05/08 15:41
L10	57	("5319712" "5754658" "6070245" "6448482" "20020083317" "20030002854" "6505299" "20030026423" "20030077071" "20030081776" "20030112333" "20030118243" "20030126086" "20030123664" "20030140257" "20030188154" "20030193973" "20030228018" "20040010717" "6684250" "20040028227" "20040081333" "20040091" "109" "20040193550" "20050071669" "6891565" "20050169473" "20050192904").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/05/08 15:41
S1	1	(authentication near2 "partial encryption" near4 "confidential message").ti.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 11:54
S2	0	"partial encryption" same set$1top$1box	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 11:55

EAST Search History

S4	0	"partial encryption" and set$1top$1box	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 11:55
S5	150	"partial encryption"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 11:56
S7	52	"partial encryption" and audio	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 11:56
S8	42	"partial encryption" same signal	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 11:57
S10	29	"partial encryption" same video	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 11:57
S11	13	"partial encryption" and audio$1video	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 12:08
S12	176	(portion near2 (encrypt$3 or encipher$3 or cipher$3 or scrambl$3)) and audio$1video	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 12:09
S13	2	"5915018".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 14:01
S14	2	"6229895".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 14:19
S15	2	"5742680".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:00

EAST Search History

S16	2	"5894516".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:02
S17	2	"5018197".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:17
S18	51	("3852519" "4381519" "4419693" "4521853" "4634808" "4700387" "4703351" "4703352" "4710811" "4722003" "4739510" "4772947" "4785361" "4788589" "4815078" "4845560" "4887296" "4890161" "4924310" "4944006" "4953023" "4995080" "5018197" "5023710").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:42
S19	57	("5122873" "5138659" "5142537" "5144662" "5159452" "5196931" "5208816" "5237424" "5241381" "5247575" "5258835" "5325432" "5327502" "5359694" "5379072" "5398078" "5416651" "5416847" "5420866" "5428403" "5434716" "5438369" "5469216" "5471501" "5473692" "5481554" "5481627").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:21
S20	54	("5485577" "5528608" "5535276" "5539823" "5539828" "5555305" "5561713" "5568552" "5574787" "5582470" "5583576" "5598214" "5600721" "5606359" "5608448" "5615265" "5617333" "5625715" "5629981" "5652795" "5663764" "5666293" "5703889" "5717814" "5732346" "5742680" "5742681").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:44
S21	55	("5751280" "5751743" "5751813" "5754650" "5757417" "5757909" "5768539" "5796786" "5796829" "5796840" "5802176" "5805700" "5805712" "5805762" "5809147" "5815146" "5818934" "5825879" "5850218" "5852290" "5852470" "5870474" "5894320" "5894516" "5915018" "5922048" "5933500").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:25

EAST Search History

S22	58	("5949877" "5949881" "5973679" "5999622" "5999698" "6005561" "6011849" "6012144" "6021199" "6021201" "6028932" "6049613" "6055314" "6057872" "6058186" "6061451" "6064748" "6065050" "6069647" "6072873" "6073122" "6088450" "6105134" "6118873" "6134551" "6154206" "6157719"). pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:54
S23	54	("6181334" "6185369" "6185546" "6189096" "6192131" "6199053" "6204843" "6209098" "6215484" "6226618" "6229895" "6230194" "6230266" "6240553" "6256747" "6263506" "6266416" "6266480" "6272538" "6278783" "6289455" "6292568" "6292892" "6307939" "6311012" "6351538" "20020046406").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:28
S24	55	("6378,130" "6389,537" "20020059425" "6389533" "6415031" "6415101" "6430361" "20020108035" "6449718" "20020129243" "6459427" "6463152" "6466671" "20020170053" "20020194613" "20020196939" "6505032" "6510554" "20030021412" "20030026423" "6519693" "6529526" "20030046686" "6543053" "20030063615" "20030081630" "20030081776").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:13
S25	51	("6587561" "20030123849" "20030123664" "20030133570" "20030145329" "20030152224" "20030152226" "20030156718" "20030159139" "20030159140" "20030159152" "20030174837" "20030198223" "6640145" "20030226149" "20040003008" "6678740" "6681326" "20040047470" "20040049688" "20040049690" "20040049691" "20040049694" "20040078575" "20040165586" "20040187161").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:31
S26	27	("8607224" "0471373" "0527611" "0558016" "0596826" "0610587" "7067028" "0680209" "9738530" "0833517" "0866615" "0031964" "0178386" "1187483" "11243534"). pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:15

EAST Search History

S27	18	("4944006" "4995080" "5555305" "6011849" "6021199" "6240553" "6292568" "6378130" "6415031"). pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:35
S28	16	("4739510" "5018197" "5247575" "5629981" "5666293" "5894516" "5915018" "6229895").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:21
S29	43	("3852519" "5325432" "5420866" "5535276" "5561713" "5742680" "5742681" "5751813" "5754650" "5518934" "5999622" "6012144" "6049613" "6055314" "6058186" "6064748" "6072873" "6307939" "20020108035" "6449718").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:23
S30	8	("1187483" "0031964" "0178386"). pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:22
S31	6	("5539823" "5600721" "6057872"). pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:38
S32	3	S18 and ((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:45
S33	5	S20 and ((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 15:54
S34	8	S22 and ((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:01
S35	12	S24 and ((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:20

EAST Search History

S36	55	("6378130" "6389537" "20020059425" "6389533" "6415031" "6415101" "6430361" "20020108035" "6449718" "20020129243" "6459427" "6463152" "6466671" "20020170053" "20020194613" "20020196939" "6505032" "6510554" "20030021412" "20030026423" "6519693" "6529526" "20030046686" "6543053" "20030063615" "20030081630" "20030081776").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:13
S37	0	S26 and ((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:21
S38	1	S28 and ((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:23
S39	11	S29 and ((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:24
S40	1	S19 and ((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:25
S41	2	S21 and ((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:26
S42	91	((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography)).ti.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:42
S43	2	multiple adj2 ((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography)).ti.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/23 16:43

EAST Search History

S44	39	multiple adj2 ((portion or partial) near2 (encryption or encipher$3 or cipher$3 or scrambl$4 or cryptography))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 12:16
S45	2	"5999622".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 12:18
S46	2	"6456985".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 12:19
S47	2	"5598470".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 12:20
S48	3	"6449718".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 12:21
S49	2	"5933499".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 15:58
S50	232	"31964"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 15:59
S51	52	"0031964"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 16:00
S52	0	wo-031964-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 16:00
S53	0	wo-31964-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 16:00

EAST Search History

S54	0	wo-0031964-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 16:00
S55	0	ep-0031964-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 16:01
S56	0	ep-031964-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 16:01
S57	1	ep-31964-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/24 16:01
S59	10	("5940738" "5973722" "20020083438" "20020196939" "20040139337").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/11 11:16
S60	2	"6292568".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/11 11:33
S61	2	"6005938".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/11 11:20
S62	2	("5870474").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/11 11:20
S64	2	"5742677".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/11 11:20
S66	13	"032228"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/11 12:11

EAST Search History

S67	0	ep-032228-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/11 11:35
S68	0	032228-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/11 11:35
S69	2	10/602,986	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/11 12:16
S71	2	"6424717".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/07/11 12:19
S72	2	"6424714".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/07/11 12:24
S75	2	"20030026423".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/07/11 12:25
S76	16	"multiple selective encryption"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/11/18 08:20
S77	22	"multiple partial encryption"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/11/18 08:21
S78	0	"multiple partial encryption" same duplicate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/11/18 08:21
S79	4	("20020150239" "6138237").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 09:01

EAST Search History

S80	5	("6549229" "6904520").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 09:08
S81	48	segment$4 same encrypt$4 same duplicat$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 09:38
S82	13	segment$4 same encrypt$4 same replicat$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 09:38
S83	2	"elementary stream" same "system information" same audio$1video	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/11/21 08:47
S84	0	ep-02806702-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/11/21 16:24
S85	1	ep-806702-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2005/11/22 13:19
S89	798	(transmit$4 or send$4 or provid$4) same (duplicat$4) same (encrypt$4 or $2cipher$4 or scramb$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/03/23 12:32
S90	30	(transmit$4 or send$4 or provid$4) same (duplicat$4) same ((encrypt$4 or $2cipher$4 or scramb$4) near9 different near9 (key or method))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/03/23 12:34

```
File   8:Ei Compendex(R) 1970-2006/Apr W4
         (c) 2006 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2006/Apr
         (c) 2006 ProQuest Info&Learning
File  65:Inside Conferences 1993-2006/May 03
         (c) 2006 BLDSC all rts. reserv.
File   2:INSPEC 1898-2006/Apr W4
         (c) 2006 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2006/Feb W1
         (c)2006 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2006/Apr W4
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2006/Apr W2
         (c) 2006 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Apr W4
         (c) 2006 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Mar
         (c) 2006 The HW Wilson Co.
File 266:FEDRIP 2005/Dec
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2006/Apr W5
         (c) 2006 FIZ TECHNIK
File  62:SPIN(R) 1975-2006/Mar W1
         (c) 2006 American Institute of Physics
File 239:Mathsci 1940-2006/Jun
         (c) 2006 American Mathematical Society

Set     Items   Description
S1      52835   ENCRYPT??? OR ENCIPHER??? OR CIPHER??? OR SCRAMBL???
S2      15462   S1(3N)(KEY? ? OR METHOD? ? OR METHODOLOG??? OR PROCEDURE? ?
                 OR ALGORITHM? ? OR SYSTEM? ? OR LOGIC OR FORMULA?? OR APPROA-
                CH OR MANNER OR MECHANISM? ?)
S3       8798   S1(3N)(TECHNIQUE? ? OR PROCESS OR PROCESSES OR FUNCTION? ?
                OR SCHEME? ? OR ROUTINE? ? OR WAY? ? OR MODE? ?)
S4     942998   (SECOND OR 2ND OR DIFFERENT OR SEPARATE OR ANOTHER OR OTHER
                 OR ALTERNATE OR ALTERNATIVE)(3W)(KEY? ? OR METHOD? ? OR METH-
                ODOLOG??? OR PROCEDURE? ? OR ALGORITHM? ? OR SYSTEM? ? OR LOG-
                IC OR FORMULA?? OR APPROACH OR MANNER)
S5     778483   (SECOND OR 2ND OR DIFFERENT OR SEPARATE OR ANOTHER OR OTHER
                 OR ALTERNATE OR ALTERNATIVE)(3W)(MECHANISM? ? OR TECHNIQUE? ?
                 OR PROCESS OR PROCESSES OR FUNCTION? ? OR SCHEME? ? OR ROUTI-
                NE? ? OR WAY? ? OR MODE? ?)
S6    2476500   IDENTICAL?? OR DUPLICAT??? OR REPLICA????? OR MATCH??? OR -
                COPY??? OR COPIES
S7     158929   S6(5N)(DATA OR INFORMATION OR CONTENT? ? OR OBJECT? ? OR F-
                ILE? ? OR DOCUMENT? ? OR ARTICLE? ? OR TEXT OR AUDIO OR MUSIC
                OR SONG? ? OR SOUND OR TRACK? ? OR CLIP? ? OR IMAGE? ? OR PIC-
                TURE? ? OR GRAPHIC? ? OR VIDEO? ? OR MOVIE? ?)
S8      68728   S6(5N)(SEGMENT? ? OR PORTION? ? OR BLOCK? ? OR SECTION? ? -
                OR PIECE? ? OR PART OR PARTS OR FRAGMENT? ? OR ITEM? ? OR ELE-
                MENT? ? OR PAGE? ? OR WEBPAGE? ?)
S9     151745   S4:S5(10N)(DATA OR INFORMATION OR CONTENT? ? OR OBJECT? ? -
                OR FILE? ? OR DOCUMENT? ? OR ARTICLE? ? OR TEXT OR AUDIO OR M-
                USIC OR SONG? ? OR SOUND OR TRACK? ? OR CLIP? ? OR IMAGE? ? OR
                 PICTURE? ? OR GRAPHIC? ? OR VIDEO? ? OR MOVIE? ?)
S10     64740   S4:S5(10N)(COPY OR COPIES OR SEGMENT? ? OR PORTION? ? OR B-
                LOCK? ? OR SECTION? ? OR PIECE? ? OR PART OR PARTS OR FRAGMEN-
                T? ? OR ITEM? ? OR ELEMENT? ? OR PAGE? ? OR WEBPAGE? ?)
S11        15   S2:S3 AND S7:S8 AND S9:S10
S12        12   RD  (unique items)
```

12/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

07878598 E.I. No: EIP06089718929
Title: Secret image sharing with smaller shadow images
Author: Wang, Ran-Zan; Su, Chin-Hui
Corporate Source: Department of Computer and Communication Engineering Ming Chuan University, Kwei-Shan, Tau-yuan, 333, Taiwan
Source: Pattern Recognition Letters v 27 n 6 Apr 15 2006. p 551-555
Publication Year: 2006
ISSN: 0167-8655
DOI: 10.1016/j.patrec.2005.09.021
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical); X; (Experimental)
Journal Announcement: 0603W1
Abstract: Secret image sharing is a technique for protecting images that involves the dispersion of the secret image into many shadow images. This endows the method with a higher tolerance against **data** corruption or loss than other **image** -protection **mechanisms** , such as **encryption** or steganography. In the method proposed in this study, the difference image of the secret image is encoded using Huffman coding scheme, and the arithmetic calculations of the sharing functions are evaluated in a power-of-two Galois Field GF(2**t). Experiment results show that each generated shadow image in the proposed method is about 40% smaller than that of the method in left bracket Thien, C.C., Lin, J.C., 2002. Secret image sharing. Comput. Graphics 26 (1), 765-770 right bracket , which improves its efficiency in storage, transmission, and **data** hiding. **copy** 2005 Elsevier B.V. All rights reserved. 14 Refs.
Descriptors: *Image processing; Pattern recognition; Cryptography
Identifiers: Steganography; Huffman coding; Data corruption
Classification Codes:
723.2 (Data Processing); 723.5 (Computer Applications); 741.1 (Light & Optics)
723 (Computer Software, Data Handling & Applications); 741 (Light, Optics & Optical Devices)
72 (COMPUTERS & DATA PROCESSING); 74 (LIGHT & OPTICAL TECHNOLOGY)

12/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

07692864 E.I. No: EIP05459458486
Title: Cross-talk-free double-image encryption and watermarking with amplitude-phase separate modulations
Author: Meng, X.F.; Cai, L.Z.; He, M.Z.; Dong, G.Y.; Shen, X.X.
Corporate Source: Department of Optics Shandong University, Jinan 250100, China
Source: Journal of Optics A: Pure and Applied Optics v 7 n 11 Nov 1 2005. p 624-631
Publication Year: 2005
CODEN: JOAOF8 ISSN: 1464-4258
Language: English
Document Type: JA; (Journal Article) Treatment: X; (Experimental)
Journal Announcement: 0511W3
Abstract: A novel digital **method** of double-image **encryption** and watermarking by constructing a complex field with one non-negative image as its amplitude and another as its phase and then encrypting this complex field by means of digital optics, such as phase-shifting interferometry with double-random phase encoding, is proposed. Since no direct addition of the information of two hidden images is employed in the **encryption process** , each image can be perfectly retrieved without cross-talk caused by the existence of the other. The feasibility of this method and its

robustness against occlusion and additional noise from watermarked images with different weighting factors are verified by computer simulations. The signal-to-noise ratio and mean square error of the retrieved **images** are calculated for **different** distortions. This **technique** can considerably improve the efficiency of **data** transmission, and it is particularly suitable for the **image** transmission via the Internet. **copy** 2005 IOP Publishing Ltd. 29 Refs.

Descriptors: *Image analysis; Cryptography; Watermarking; Holographic interferometry; Image processing; Image reconstruction; Computer simulation ; Internet; Phase shift

Identifiers: Image encryption and watermarking; Mean square error; Double-random phase encoding; Watermarked images

Classification Codes:

723.2 (Data Processing); 743.2 (Holographic Applications); 723.5 (Computer Applications); 703.1 (Electric Networks)

723 (Computer Software, Data Handling & Applications); 741 (Light, Optics & Optical Devices); 743 (Holography); 703 (Electric Circuits)

72 (COMPUTERS & DATA PROCESSING); 74 (LIGHT & OPTICAL TECHNOLOGY); 70 (ELECTRICAL ENGINEERING, GENERAL)

12/5/3 (Item 3 from file: 8)

07488022 E.I. No: EIP05289200344

Title: Efficient state updates for key management

Author: Pinkas, Benny

Corporate Source: HP Labs, Princeton, NJ 08540, United States

Source: Proceedings of the IEEE Enabling Security Technologies for Digital Richts Management v 92 n 6 June 2004. p 910-917

Publication Year: 2004

CODEN: IEEPAD ISSN: 0018-9219

Language: English

Document Type: JA; (Journal Article) Treatment: T; (Theoretical)

Journal Announcement: 5073W205073 left bracket 7-7 right bracket

Abstract: Encryption is widely used to enforce usage rules for digital content. In many scenarios content is **encrypted** using a group **key** which is known to a group of users that are allowed to use the content. When users leave or join the group, the group key must be changed. The logical key hierarchy (LKH) algorithm is a very common method of managing these key changes. In this algorithm every user keeps a personal key composed of log n keys (for a group of n users). A key update message consists of O(log n) keys. A major drawback of the LKH algorithm is that users must update their state whenever users join or leave the group. When such an event happens, a key update message is sent to all users. A user who is offline during t key updates, and who needs to learn the keys sent in these updates as well as update its personal key, should receive and process the t key update messages, of total length O(t log n) keys. In this paper we show how to reduce this overhead to a message of O(log t) keys. We also note that one of the methods that are used in this work to reduce the size of the update message can be used is other scenarios as well. It enables one to generate n pseudorandom keys of length k bits each, such that any successive set oft keys can be represented by a string log(t) center dot k bits, without disclosing any **information** about the **other keys** . **copy** 2004 IEEE. 18 Refs.

Descriptors: *Public key cryptography; Information management; Hierarchical systems; Servers; Digital communication systems; Algorithms; Computational geometry

Identifiers: Broadcast encryption; Digital rights management (DRM); Revocation; Logical key hierarchy (LKH)

Classification Codes:

903.2 (Information Dissemination); 731.1 (Control Systems); 723.5 (Computer Applications); 921.4 (Combinatorial Mathematics, Includes Graph Theory, Set Theory)

716 (Electronic Equipment, Radar, Radio & Television); 903 (Information Science); 731 (Automatic Control Principles & Applications); 722 (Computer Hardware); 723 (Computer Software, Data Handling & Applications); 921 (Applied Mathematics)
71 (ELECTRONICS & COMMUNICATION ENGINEERING); 90 (ENGINEERING, GENERAL); 73 (CONTROL ENGINEERING); 72 (COMPUTERS & DATA PROCESSING); 92 (ENGINEERING MATHEMATICS)

12/5/4 (Item 4 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

06452845 E.I. No: EIP03297550548
Title: A temporal key management scheme for secure broadcasting of XML documents
Author: Bertino, Elisa; Carminati, Barbara; Ferrari, Elena
Corporate Source: DSI Universita di Milano, Milano, Italy
Conference Title: Proceedings of the 9th ACM Conference on Computer and Communications Security
Conference Location: Washington, DC, United States Conference Date: 20021118-20021122
Sponsor: ACM SIGSAC
E.I. Conference No.: 61154
Source: Proceedings of the ACM Conference on Computer and Communications Security 2002. p 31-40
Publication Year: 2002
Language: English
Document Type: CA; (Conference Article) Treatment: G; (General Review)
Journal Announcement: 0307W4
Abstract: Secure broadcasting of web documents is becoming a crucial need for many web-based applications. Under the broadcast document dissemination strategy a web document source periodically broadcasts (portions of) its documents to a possibly large community of subjects, without the need of explicit subject requests. By secure broadcasting we mean that the delivery of information to subjects must obey the access control policies of the document source. Since different subjects may have the right to access different portions of the same document, enforcing secure broadcasting requires to efficiently manage a large number of different physical views of the requested document and sending them to the proper subjects. In this paper we present an approach to secure broadcasting of web documents, based on the use of **encryption techniques** , and supporting the specification of fine-grained temporal access control policies. The idea is to generate a unique encrypted **copy** of the **document** to be released, where different **portions** of the **document** are **encrypted** with **different keys** , on the basis of the specified access control policies. Each subject then obtains the secret keys corresponding to document portions he/she is authorized to access. The key aspect of our approach is that the number of keys to be generated does not depend on the number of subjects nor on the document dimension, but only on the number of specified access control policies and the associated temporal constraints. 11 Refs.
Descriptors: *Security of data; Broadcasting; XML; Electronic document exchange; World Wide Web; Cryptography; Data acquisition; Constraint theory; Database systems
Identifiers: Temporal key management; Broadcast document dissemination; Access control policies
Classification Codes:
723.1.1 (Computer Programming Languages)
723.2 (Data Processing); 716.1 (Information & Communication Theory); 723.1 (Computer Programming); 723.5 (Computer Applications); 721.1 (Computer Theory (Includes Formal Logic, Automata Theory, Switching Theory & Programming Theory)); 723.3 (Database Systems)
723 (Computer Software, Data Handling & Applications); 716 (Electronic Equipment, Radar, Radio & Television); 721 (Computer Circuits & Logic

Elements)
  72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATION ENGINEERING)

12/5/5 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01734019 ORDER NO: AADAA-I9960726
The all-digital ring-wedge detector applied to automatic object recognition
  Author: Berfanger, David M.
  Degree: Ph.D.
  Year: 2000
  Corporate Source/Institution: The University of Rochester (0188)
  Supervisor: Nicholas George
  Source: VOLUME 61/02-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
  PAGE 914. 162 PAGES
  Descriptors: PHYSICS, OPTICS ; COMPUTER SCIENCE ; ARTIFICIAL INTELLIGENCE
  Descriptor Codes: 0752; 0984; 0800

An all-digital ring-wedge detector is presented, which when coupled with neural network software produces a highly flexible recognition system, sharing many of the advantages of the optoelectronic hybrid system for obtaining the same data format. While less capable in terms of space-bandwidth product, the all-digital system is relatively simple to use, much less expensive, and readily applicable both with hard- **copy images** and digital **images** , offering the possibility of interesting variations on what one is able to do with the hybrid system.

Several problems dealing with automatic object recognition are studied with contributions including the first detailed descriptions of two **separate algorithms** for calculating the ring-wedge **data** format. Also, the use of spatial frequency domain information in combination with image domain information for improved recognition is emphasized through the introduction of a novel localized ring-wedge transform, which extracts localized spatial frequency information as a function of position within a larger scene.

In fingerprint recognition we demonstrate a very effective system applicable with either gray-scale or binary images, including ring-only (orientation independent) and wedge-only (scale-size independent) sortings. Further, we present a successful fingerprint verification system based on a user carrying a data **encrypted key** and being allowed entrance by comparing stored data to data collected directly from the subject's fingerprint. In the application of the localized ring-wedge transform to fingerprint imagery, direct examples are presented demonstrating fingerprint quality detection and local ridge orientation determination.

In the operator-independent, automatic assessment of image quality, we report a high accuracy in the classification of both linear (image blur level) and nonlinear (image compression artifacts) degradations in a manner that is widely independent of scene content. Using interesting system variations, we present several experiments in which the end goal is to classify images according to numerical quality scales. In addition, the localized ring-wedge transform is found to be valuable for estimating local perceptual fidelity. We emphasize that our method is using information from the degraded image alone, without specific data from the original scene; however, the original scene can be incorporated as a reference when appropriate.

12/5/6 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

09652568

Title: Increasing distributed storage survivability with a stackable RAID-like file system
Author(s): Joukov, N.; Rai, A.; Zadok, E.
Author Affiliation: State Univ. of New York, Stony Brook, NY, USA
Conference Title: 2005 IEEE International Symposium on Cluster Computing and the Grid (IEEE Cat. No. 05EX1055) Part Vol. 1 p.82-9 Vol. 1
Publisher: IEEE, Piscataway, NJ, USA
Publication Date: 2005 Country of Publication: USA 2 vol. (xxii+1158) pp.
ISBN: 0 7803 9074 1 Material Identity Number: XX-2005-01465
U.S. Copyright Clearance Center Code: 0 7803 9074 1/2005/$20.00
Conference Title: 2005 IEEE International Symposium on Cluster Computing and the Grid
Conference Date: 9-12 May 2005 Conference Location: Cardiff, Wales, UK
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: We have designed a stackable file system called Redundant Array of Independent Filesystems (RAIF). It combines the data survivability properties and performance benefits of traditional RAIDs with the unprecedented flexibility of composition, improved security, and ease of development of stackable file systems. RAIF can be mounted on top of any combination of **other file systems** including network, distributed, disk-based, and memory-based **file systems** . Existing **encryption** , compression, antivirus, and consistency checking stackable file systems can be mounted above and below RAIF, to efficiently cope up with slow or unsecure branches. Individual **files** can be distributed across branches, **replicated** , stored with parity, or stored with erasure correction coding to recover from failures on multiple branches. Per-file incremental recovery, storage type migration, and load-balancing are especially well suited for grid storages. In this paper, we describe the current RAIF design, provide preliminary performance results and discuss current status and future directions. (34 Refs)
Subfile: C
Descriptors: distributed databases; network operating systems; parallel processing; RAID
Identifiers: distributed storage survivability; stackable RAID-like file system; Redundant Array of Independent Filesystems; RAIF; network file systems; distributed file systems; disk-based file systems; memory-based file systems; **encryption** stackable file **systems** ; compression stackable file systems; antivirus stackable file systems; consistency checking stackable file systems; erasure correction coding; per-file incremental recovery; storage type migration; load-balancing; grid storages
Class Codes: C5320C (Storage on moving magnetic media); C5440 (Multiprocessing systems); C6150N (Distributed systems software)

12/5/7 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

09306159 INSPEC Abstract Number: B2005-04-6135E-052, C2005-04-1250M-064
Title: Digital passport system
Author(s): Pramsane, S.; Tran Duc Hai Du
Author Affiliation: Sch. of Internet & E-Commerce Technol., Assumption Univ., Thailand
Conference Title: Proceedings of the 2004 International Conference on Information and Communication Technologies (ICT 2004) p.150-7
Editor(s): Batovski, D.A.; Fedoseev, S.A.
Publisher: Assumption Univ, Bangkok, Thailand
Publication Date: 2004 Country of Publication: Thailand viii+284 pp.
ISBN: 974 615 191 6 Material Identity Number: XX-2005-00367
Conference Title: Proceedings of the 2004 International Conference on Information and Communication Technologies (ICT 2004)
Conference Date: 18-19 Nov. 2004 Conference Location: Bangkok,

Thailand
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P); Experimental (X)
Abstract: This paper proposes a new system that could be used instead of the current passport by using fingerprint, face recognition, and data encryption. This paper describes a simple algorithm which allows the creation of a sample image from a face recognition and fingerprint **image** template using a **match** score value. In this paper, face recognition (1) and fingerprint (2) are two **different systems** , and hold different types of **information** : (1) original **information** and (2) encryption information. The encryption information is the original information encrypted by AES (advanced encryption standard). After verification of the face and fingerprint, this data must be verified again for its consistency. The regenerated image compares with a high score to the original image, and visually shows most of the essential features. This image could thus be used to fool the algorithm as the target person, or visually identify that individual. Importantly, this algorithm is immune to template **encryption** : any **system** which allows access to **match** scores effectively allows sample **images** to be regenerated in this way. (11 Refs)
Subfile: B C
Descriptors: cryptography; face recognition; fingerprint identification; **image matching** ; image reconstruction
Identifiers: biometrics passport; digital passport system; fingerprint recognition; face recognition; data encryption; fingerprint image template; match score value; AES encrypted information; advanced encryption standard; image regeneration; template encryption
Class Codes: B6135E (Image recognition); B6120D (Cryptography); C1250M (Image recognition); C5260B (Computer vision and image processing techniques); C6130S (Data security)

12/5/8 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

09212236 INSPEC Abstract Number: C2005-01-6170K-099
Title: Blind data linkage using n-gram similarity comparisons
Author(s): Churches, T.; Christen, P.
Author Affiliation: Dept. of Health, New South Wales Univ., Sydney, NSW, Australia
Conference Title: Advances in Knowledge Discovery and Data Mining. 8th Pacific-Asia Conference, PAKDD 2004. Proceedings (Lecture Notes in Artificial Intelligence Vol.3056) p.121-6
Editor(s): Dai, H.; Srikant, R.; Zhang, C.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 2004 Country of Publication: Germany xix+713 pp.
ISBN: 3 540 22064 X Material Identity Number: XX-2004-01272
Conference Title: Advances in Knowledge Discovery and Data Mining. 8th Pacific-Asia Conference, PAKDD 2004. Proceedings
Conference Sponsor: SAS; Univ of Technol, Sydney
Conference Date: 26-28 May 2004 Conference Location: Sydney, NSW, Australia
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Integrating or linking data from different sources is an increasingly important task in the preprocessing stage of many data mining projects. The aim of such linkages is to merge all records relating to the same entity, such as a patient or a customer. If no common unique entity identifiers (keys) are available in all data sources, the linkage needs to be performed using the available identifying attributes, like names and addresses. Data confidentiality often limits or even prohibits successful data linkage, as either no consent can be gained (for example in biomedical studies) or the data holders are not willing to release their **data** for linkage by **other** parties. We present **methods** for confidential **data**

linkage based on hash encoding, public **key encryption** and n-gram similarity comparison techniques, and show how blind data linkage can be performed. (10 Refs)
Subfile: C
Descriptors: data mining; data privacy; database indexing; encoding; merging; public key cryptography
Identifiers: blind data linkage; n-gram similarity comparison; data mining; entity identifier; data source; hash encoding; public **key encryption** ; data privacy; **data matching**
Class Codes: C6170K (Knowledge engineering techniques); C6130 (Data handling techniques); C6160 (Database management systems (DBMS)); C6130S (Data security)

12/5/9 (Item 4 from file: 2)

08404274 INSPEC Abstract Number: C2002-11-6150N-125
Title: Reclaiming space from duplicate files **in a serverless distributed** file **system**
Author(s): Douceur, J.R.; Adya, A.; Bolosky, W.J.; Simon, P.; Theimer, M.
Conference Title: Proceedings 22nd International Conference on Distributed Computing Systems p.617-24
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 2002 Country of Publication: USA xx+627 pp.
ISBN: 0 7695 1585 1 Material Identity Number: XX-2002-02283
U.S. Copyright Clearance Center Code: 1063-6927/02/$17.00
Conference Title: Proceedings 22nd International Conference on Distributed Computing Systems
Conference Sponsor: IEEE Comput. Tech. Committee on Distributed Process. (TCDP)
Conference Date: 2-5 July 2002 Conference Location: Vienna, Austria
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T); Experimental (X)
Abstract: The Farsite distributed **file** system provides availability by **replicating** each **file** onto multiple desktop computers. Since this replication consumes significant storage space, it is important to reclaim used space where possible. Measurement of over 500 desktop file systems shows that nearly half of all consumed space is occupied by **duplicate files** . We present a mechanism to reclaim space from this incidental duplication to make it available for controlled **file replication** . Our **mechanism** includes: (1) convergent **encryption** , which enables **duplicate files** to be coalesced into the space of a single **file** , even if the **files** are **encrypted** with **different** users' **keys** ; and (2) SALAD, a Self-Arranging Lossy Associative Database for aggregating file content and location information in a decentralized, scalable, fault-tolerant manner. Large-scale simulation experiments show that the **duplicate - file** coalescing system is scalable, highly effective, and fault-tolerant. (40 Refs)
Subfile: C
Descriptors: content-addressable storage; cryptography; network operating systems; replicated databases; self-organising storage; software fault tolerance; storage management
Identifiers: Farsite; availability; storage space reclamation; desktop file systems; **duplicate files** ; controlled **file replication** ; convergent encryption; SALAD; file content aggregation; Self-Arranging Lossy Associative Database; location information; decentralized scalable system; fault-tolerant system; large-scale simulation; **duplicate - file** coalescing system; serverless distributed file system
Class Codes: C6150N (Distributed systems software); C6120 (File organisation); C6160B (Distributed databases); C6130S (Data security)

12/5/10 (Item 5 from file: 2)
DIALOG(R)File 2:INSPEC

06807583 INSPEC Abstract Number: B9802-6140C-420, C9802-5260B-268
Title: Digital image scrambling method **for information distribution**
Author(s): Fujii, H.; Yamanaka, Y.
Journal: Transactions of the Information Processing Society of Japan vol.38, no.10 p.1945-55
Publisher: Inf. Process. Soc. Japan,
Publication Date: Oct. 1997 Country of Publication: Japan
CODEN: JSGRD5 ISSN: 0387-5806
SICI: 0387-5806(199710)38:10L.1945:DISM;1-C
Material Identity Number: T205-97012
Language: Japanese Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: During the distribution of digital images, protection against piracy is important because it is easy to **duplicate** digital **data** without deterioration and to spread pirated versions through networks. Providers of image data cannot disclose the original data for fear of piracy, yet still need to advertise their products and to allow customers to evaluate a product prior to paying for it. The paper presents a **method** for **scrambling** image data encoded in JPEG or MPEG1 in order to solve this problem. Our **method** uses a **cipher algorithm** for data transformation to generate a deteriorated version of the image data. Its high speed transformation enables real time descrambling, thereby preventing illegal copying. For effective advertisements and copyright protection, the degree to which image data is scrambled should be controllable. Using our **method** , **scrambling** can be controlled by the intra block parameters, density and area. The method also allows a single **image** to be scrambled a number of times using **different scrambling keys** . Multiple **scrambling** can be used to determine the **image** quality based on the level of payment. It can also be used to protect image data composed of several parts, the copyright for each part being owned by different authors. (17 Refs)
Subfile: B C
Descriptors: copyright; cryptography; image coding; real-time systems
Identifiers: digital image **scrambling method** ; information distribution; digital image distribution; piracy; image data protection; JPEG; MPEG1; **cipher algorithm** ; data transformation; deteriorated version; high speed transformation; real time descrambling; illegal copying ; advertisements; copyright protection; intra block parameters; **scrambling keys** ; multiple scrambling; image quality
Class Codes: B6140C (Optical information, image and video signal processing); B6120B (Codes); C5260B (Computer vision and image processing techniques); C6130S (Data security)

12/5/11 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus

03205837 JICST ACCESSION NUMBER: 97A0589508 FILE SEGMENT: JICST-E
Image Semi-disclosure Method for Copyright Protection.
ABE TAKEHITO (1); FUJII HIROSHI (1); KUSHIMA KAZUHIKO (1)
(1) NTT Information and Communication System Lab.
Eizo Joho Media Gakkai Gijutsu Hokoku, 1997, VOL.21,NO.31(VIR97 23-29), PAGE.9-14, FIG.8, REF.9
JOURNAL NUMBER: S0209ABW ISSN NO: 1342-6893
UNIVERSAL DECIMAL CLASSIFICATION: 681.3.02-759 681.3:621.397.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper

MEDIA TYPE: Printed Publication
ABSTRACT: During the distribution of digital images, protection against piracy is important because it is easy to **duplicate** digital **data** without deterioration and to spread pirated versions through networks. This paper presents a **method** for **scrambling** image data encoded in JPEG. Our **method** uses a **cipher algorithm** for data transformation. Its high-speed transformation enables real time descrambling, thereby preventing illegal copying. Using our **method** , **scrambling** can be controlled by the intra-block parameters, density and area. The method also allows a single **image** to be scrambled a number of times using **different scrambling keys** . Besides we propose an **image** distribution **method** using **scrambled images** with our experimental tools. (author abst.)
DESCRIPTORS: data protection; moving image; digital image; cryptogram; computer security; copyright; scrambler
BROADER DESCRIPTORS: protection; image; security; guarantee; intellectual property; right; signal converter; electric converter; converter; communication apparatus; equipment
CLASSIFICATION CODE(S): JD01020V; JE04010I

12/5/12 (Item 2 from file: 94)
DIALOG(R)File 94:JICST-EPlus

03120824 JICST ACCESSION NUMBER: 97A0245209 FILE SEGMENT: JICST-E
Digital Image Scrambling Method **for Copyright Protection.**
FUJII HIROSHI (1); KUSHIMA KAZUHIKO (1)
(1) NTT Information and Communication System Lab.
Joho Shori Gakkai Kenkyu Hokoku, 1997, VOL.97,NO.13(DPS-80 GW-21), PAGE.49-54, FIG.8, REF.10
JOURNAL NUMBER: Z0031BAO ISSN NO: 0919-6072
UNIVERSAL DECIMAL CLASSIFICATION: 681.3.02-759 681.3:621.397.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: During the distribution of digital images, protection against piracy is important because it is easy to **duplicate** digital **data** without deterioration and to spread pirated versions through networks. This paper presents a **method** for **scrambling** image data encoded in JPEG. Our **method** uses a **cipher algorithm** for data transformation. Its high-speed transformation enables real time descrambling, thereby preventing illegal copying. Using our **method** , **scrambling** can be controlled by the intra-block parameters, density and area. The method also allows a single **image** to be scrambled a number of times using **different scrambling keys** . Multiple **scrambling** can be used to determine the **image** quality based on the level of payment. It can also be used to protect image data composed of several parts, the copyright for each part being owned by different authors. (author abst.)